Abc -Empresa Suplemento
Fecha: domingo, 07 de junio de 2026
Fecha Publicación: domingo, 07 de junio de 2026
Página: 10, 11
Nº documentos: 2

Recorte en color % de ocupación: 175,03 Valor: 63616,97€ Periodicidad: Diaria Tirada: 54.907 Audiencia: 364.000 Difusión: 34.952

Europa busca un escudo integral para blindar su sistema energético frente a la amenaza del ciberdelito

Los avances regulatorios son un primer paso para crear una respuesta homogénea y coordinada que aumente la resiliencia de unas infraestructuras críticas asediadas por el incremento de ataques

Charro Barroso

El 20 de enero de 2026, la Comisión Europea presentó un nuevo y amplio paquete con el propósito de reforzar la resiliencia y las capacidades de ciberseguridad de la Unión Europea, en respuesta al creciente número de amenazas cibernéticas e híbridas que afectan a los servicios esenciales. La propuesta incluye la revisión del Reglamento de Ciberseguridad (Cybersecurity Act) y modificaciones específicas de la Directiva NIS2.

Un reciente informe de TrendAI, unidad de negocio de Trend Micro, advierte del uso intensivo de la IA en los ciberataques, por lo que aconseja a las organizaciones que abandonen los modelos enfocados en la prevención y adopten otros basados en visibilidad, contención y recuperación rápida. El estudio muestra que en 2025 los ciberataques al sector energético crecieron un 113%. José de la Cruz, director técnico de TrendAI, comenta que un ciberataque a infraestructuras críticas puede provocar un enorme impacto: «No solo económico. Si se interrumpe el servicio de una región o de un país, el daño es global. Afecta a usuarios, a empresas... Tiene muchos vectores posibles de ataque, como a través del suministro local, con el robo de datos, o contra la propia estructura». Estima De la Cruz que el gran apagón que sufrió España en abril de 2025, a pesar de no tener nada que ver con un ciberataque, «ha ayudado a mejorar las barreras, a elevar las alertas contra las ciberamenazas».

La actividad de los grupos APT (Amenaza Persistente Avanzada), con frecuencia auspiciados por Estados, ha experimentado un importante incremento en los últimos tiempos. Estas campañas no tienen como principal objetivo la interrupción del flujo de energía. Pretenden, sobre todo, información sobre redes eléctricas. Se dedican por eso en las fases iniciales al reconocimiento, el robo de credenciales y el posicionamiento dentro de los sistemas. Es la fórmula para mantener acceso a largo plazo y preparar posibles acciones futuras.

Mantiene De la Cruz que el blindaje frente a estos grupos de amenaza debe ser de las mismas características que la protección genérica: «Existen dos corrientes de ataque, unos buscan un rédito económico y otros tienen un fin ideológico, político o están contratados. Aunque estos últimos pudieran tener más fondos y herramientas más sofisticadas, los métodos son muy similares». La ciberseguridad es una cuestión de iniciativa, relata: «Resulta importante tener una estrategia más proactiva, no solamente estar a la espera de que nos ataquen para responder, sino también identificar cuáles son los puntos débiles, al menos para mitigarlos».

En evolución

El nuevo paradigma de la seguridad está marcado por la evolución. «Europa tiene como objetivo primordial aumentar la resiliencia. Toda la regulación ha estado muy marcada por lo físico, pero ahora lo digital se sitúa al mismo nivel», indica Marta Castro, directora de Regulación de la Asociación de Empresas de Energía Eléctrica (Aelec). Con unas redes eléctricas cada vez más digitalizadas y conectadas, «Europa está impulsando la armonización de estándares entre países», menciona. Porque la ciberseguridad ya no consiste simplemente en «comprar un programa informático», se trata, según Castro, de «un proceso integral de protección de las infraestructuras que hacen posible que la electricidad llegue a los hogares y a las empresas».

Un solo eslabón vulnerable puede generar impactos sistémicos

Los ciberataques al sector crecieron un 113% en 2025, según Trend AI

El sector eléctrico tiene particularidades que lo hacen más crítico y vulnerable que otros ámbitos por ser «un servicio esencial para la sociedad sin alternativa inmediata». Considera la directora de Regulación de Aelec que estamos ante «la infraestructura de las infraestructuras, porque cuando funciona, todo va bien, pero cuando falta nada marcha». Y se desarrolla en tiempo real: «Si falla, colapsan los hospitales, las telecomunicaciones, el agua, las gasolineras, la industria», aclara. Conflictos y situaciones como la guerra de Ucrania o las tensiones con Irán dificultan la segu-

Abc -Empresa Suplemento
Fecha: domingo, 07 de junio de 2026
Fecha Publicación: domingo, 07 de junio de 2026
Página: 10, 11
Nº documentos: 2

Recorte en color % de ocupación: 175,03 Valor: 63616,97€ Periodicidad: Diaria Tirada: 54.907 Audiencia: 364.000 Difusión: 34.952

ridad de las infraestructuras eléctricas, pero también impulsan la protección de las redes. En este sentido, Castro apuesta por definir «protocolos de actuación coordinados y sujetos a supervisión constante, unos protocolos de continuidad de negocio tanto nacionales como internacionales» para saber cómo reaccionar conjuntamente ante un cero energético provocado por un ciberataque.

Para fortalecer la protección es necesaria una inversión adecuada. De hecho, el Gobierno ya está identificando la digitalización y la resiliencia de las redes como prioridades, y para ello se aumentarán los límites de inversión permitidos para las empresas. ¿Afectará esto al bolsillo del consumidor? Estas inversiones se recuperan a través de los peajes de la luz, regulados por la CNMC. Explica Marta Castro que no tienen por qué encarecer la factura del cliente final: «Si se acompasan con un incremento de la demanda eléctrica, estas inversiones serían costo-eficientes».

La óptica gasista

La propuesta de revisión del marco europeo ha sido valorada por el sector gasista español. Desde la Asociación Española del Gas (Sedigas), aseguran que «la ciberseguridad no puede dejar huecos en la cadena de valor: un solo eslabón vulnerable, por pequeño que sea, puede generar impactos sistémicos y provocar daños significativos». «De ahí la importancia de que el enfoque europeo sea integral, homogéneo y coordinado, abarcando desde grandes infraestructuras hasta operadores de menor tamaño», apuntan.

«El gas, y cada vez más el gas renovable, forma parte de infraestructuras esenciales para el funcionamiento de la economía y el bienestar de los ciudadanos», sostiene Sedigas. Las empresas gasistas, que ya operan bajo marcos estrictos de seguridad operativa y digital, precisarán, como el sector eléctrico, nuevas inversiones estratégicas.

La ciberseguridad pasa a ser un pilar central de la gestión empresarial y operativa del sector gasista, al mismo nivel que la seguridad física, la protección ambiental o la fiabilidad del suministro, declaran desde Sedigas: «No es solo una cuestión tecnológica, sino también organizativa y cultural; gestión integral del riesgo, formación del personal, coordinación con autoridades, planes de contingencia, simulacros, intercambio de información y cooperación europea. En un sistema energético cada vez más interconectado, digitalizado y descentralizado –con gases renovables, nuevas plantas, nuevos operadores y mayor integración sectorial–, la protección frente a ciberamenazas será un factor clave de confianza, estabilidad y competitividad de la economía».

La Directiva Europea 2022/2557 (CER) es otra herramienta que brinda la Comisión para fortalecer la capacidad de respuesta. El pasado mes de marzo, la Asociación Cluster Catástrofes y el Instituto de la Ingeniería de España (IIE) hicieron público el Manifiesto sobre la Directiva CER para reforzar la resiliencia de las infraestructuras críticas.

La protección se ha convertido en una prioridad estratégica. Jaime Segarra, secretario del Comité de Energía y Recursos Naturales del IIE, alerta del peligro que entrañan «la inteligencia artificial y el desencriptado de la computación cuántica, porque disponen de una capacidad de análisis y de penetración en sistemas exponencialmente superior a lo que se ha tenido hasta el momento».

«Si una clave necesitaba decenas de años para descifrarla con los ordenadores clásicos, con la computación cuántica y la inteligencia artificial se puede resolver en horas. La seguridad de las claves es el primer problema», añade.

Riesgos añadidos

Pero hay más riesgos: las barreras para que no penetren las ataques. «Dos son los medios clásicos de protección», explica Segarra. «Uno es impedir que los medios digitales accedan a las infraestructuras, la protección de procedimiento. Y otro es el que se emplea, por ejemplo, en las centrales nucleares, donde se utilizan barreras analógicas que no se pueden operar desde un punto exterior. Este sistema crea problemas de lentitud y aislamiento, pero hubiera evitado, por ejemplo, el bloqueo entre 2007 y 2008 de las centrifugadoras de enriquecimiento de uranio en Irán con el virus Stuxnet introducido por el Mosad, el servicio secreto israelí», asegura.

La combinación de barreras digitales y analógicas ya no sirve. «Estamos en una fase completamente incipiente porque nadie sabe muy bien hacia dónde va a evolucionar la tecnología», afirma Segarra.

La política energética en la Unión Europea es una competencia compartida entre la UE y los Estados miembros, circunstancia que puede ocasionar una falta de coordinación, señala. Sobre España, expresa que es una fortaleza «la protección de centrales eléctricas y de sistemas gasistas, gracias al regulador potente e independiente; también sucede con las centrales nucleares».